

Auditing Organizational Security

Eugene A. Razzetti

Managing organizational security is no different from managing any other of the command's missions. Establish your policies, goals and risk parameters; implement, train, measure and benchmark them. And then audit, audit, audit.

Today, more than ever, Organizational Security is an essential component of a robust, responsive military command. And commands that cannot execute their operations in a self-imposed and self-monitored secure environment may, at best, cease to be effective or, at worst, cease to exist. This is the same, certain fate that befalls private enterprises that cannot maintain operational effectiveness, profitability or product superiority—except it happens faster in the private sector.

Organizations must harden their operations to protect them from either incidental or deliberate attack. Internal (or self-) auditing is essential to the hardening process.

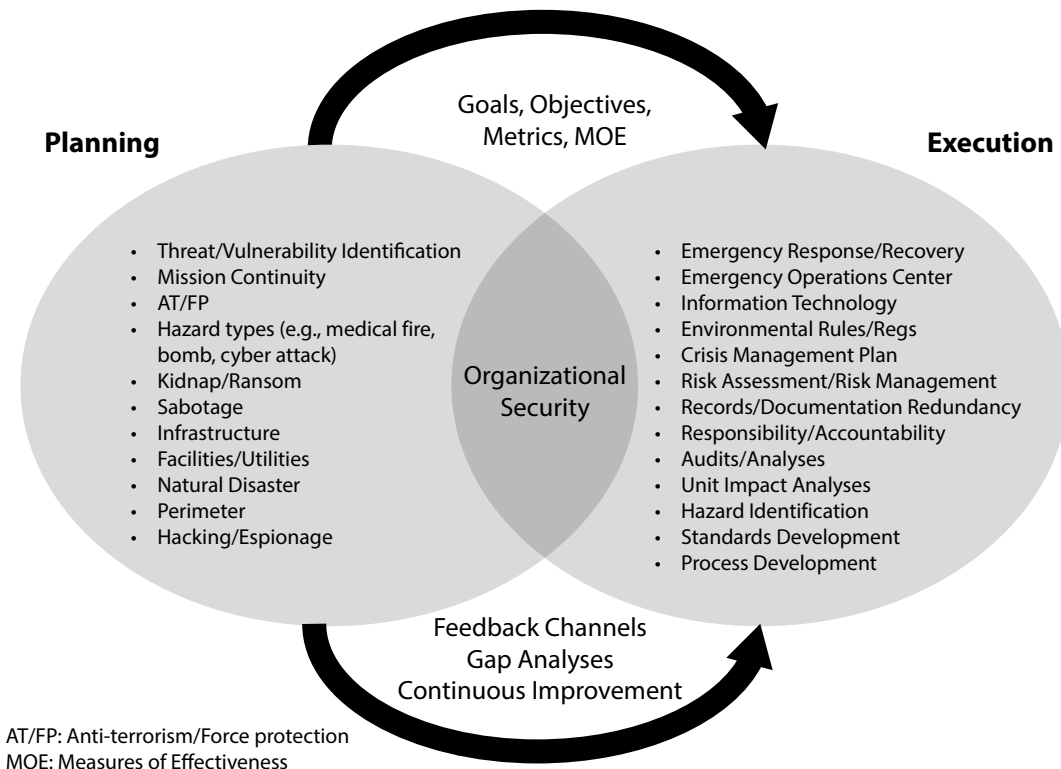
Cybersecurity, the concept most frequently promoted these days, is a body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Is cybersecurity important and necessary? Of course! However, cybersecurity should not be regarded as independent or standing alone. Cybersecurity is an indispensable element of organizational security, which is the subject of this article.

Figure 1 describes the many organizational security-related challenges that military commands (including cybersecurity) confront in moving from planning to executing their missions.

Razzetti, a retired U.S. Navy captain, is a management consultant military analyst and certification auditor. He is the author of five management books, numerous articles and analytical reports, and has served on the advisory boards of two business schools.



Figure 1. The Big Picture: Organizational Security in Mission Execution



on audit findings perpetuate continual improvement and help to establish and maintain an ongoing robust security posture. This involves eternally raising the bar and leaving the current status quo in the rearview mirror. I recommend that commanders who want to establish and maintain structured information systems security management review the following from the International Organization for Standardization (ISO): ISO 27000: *Information Systems Security Management*.

A robust program of internal auditing of a command's organizational security hardens and protects military operations under a structured organiza-

Several years ago, I worked as a military analyst on programs that included information warfare (like all modern defense programs). The lesson I continually relearned during that time was that information is the only "weapon" that can be in more than one place at the same time.

As information technology (IT) is increasingly integrated with physical infrastructure, the risk increases of wide-scale or high-consequence events that could harm or disrupt military commands and their missions. Therefore, strengthening organizational security and resilience is critical.

All U.S. military commands depend on IT systems and computer networks for essential operations and mission fulfillment. IT systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade or destroy critical information systems or to put infrastructure (e.g., power plants) out of commission.

Internal and external auditing of organizational security programs can ensure compliance with requirements and can sustain an acceptable level of impregnability. However, generating preventive and corrective actions as a result of those audits and reassessing goals and objectives based

tional security management system. Anything less than robust jeopardizes the existence of the command, the capability of its leadership and the fulfillment of its missions.

There are 10 auditable areas in which commands can create and sustain credible, effective and secure management systems and strategies—for headquarters commands, subordinates in the field and suppliers.

1. Policy Development

Commanders must develop, as applicable to the mission, written security policies that are:

- Consistent with the other policies of the organization and those of higher authority
- Specifically keyed to planned security objectives, targets, and programs
- Consistent with the organization's overall security threat and risk management strategy and the nature and scale of its operations
- Clear in stating overall/broad security management objectives
- Documented, implemented and monitored
- Communicated to all levels and to third parties, including contractors and visitors, so that they all are made aware of their security-related obligations.

Things refuse to be mismanaged long.

—Ralph Waldo Emerson

2. Program Management

Effectively managing any program requires the continual monitoring of the effectiveness of projects, procurements and suppliers, establishment of metrics and early identification of potential problems. Commands must assess all their functions and spend their limited resources according to how much their vulnerability is reduced by that expenditure, as shown in Figure 2.

As the arrows suggest, managers want to minimize funds committed to ineffective programs. The goal of the program management (with programs pictured as small pyramids) is to move programs into Quadrants II and III. Programs in Quadrant I may appear acceptable but can breed complacency, and there is no longer any room for complacency in organizational security. Programs or projects that fall into Quadrant IV are unacceptable and require forthright (and probably unwelcome) corrective action.

At the same time, commanders must establish program management roles, responsibilities and authorities that are consistent with achieving security management policies and objectives. And these must be communicated to all responsible parties.

Commanders need to make a commitment, measurably and consistently, to developing a Security Management System (SMS) and continually improving its effectiveness. This is accomplished specifically by:

- Communicating to all parts of the organization the importance of meeting security management requirements in order to comply with established policies
- Ensuring any security programs generated from other parts of the organization complement the security management system
- Establishing meaningful security metrics and measures of effectiveness
- Ensuring security-related threats, criticalities and vulnerabilities are evaluated and included in organizational risk assessments where appropriate
- Ensuring the viability of the security management objectives, targets and programs.

3. Security Risk Management

Security risk management, like any other focused risk management strategy, requires that commanders identify and assess “risk” in terms of threats, criticalities and vulnerabilities to the commands and their assigned missions. Commanders must establish and maintain strategies for the ongoing identification, assessment and mitigation of all risks, especially those related to organizational security. Mitigation means identifying and implementing effective control measures. In the execution of control measures, risk assessment becomes risk management. An effective security risk assessment strategy should include identifying (when appropriate):

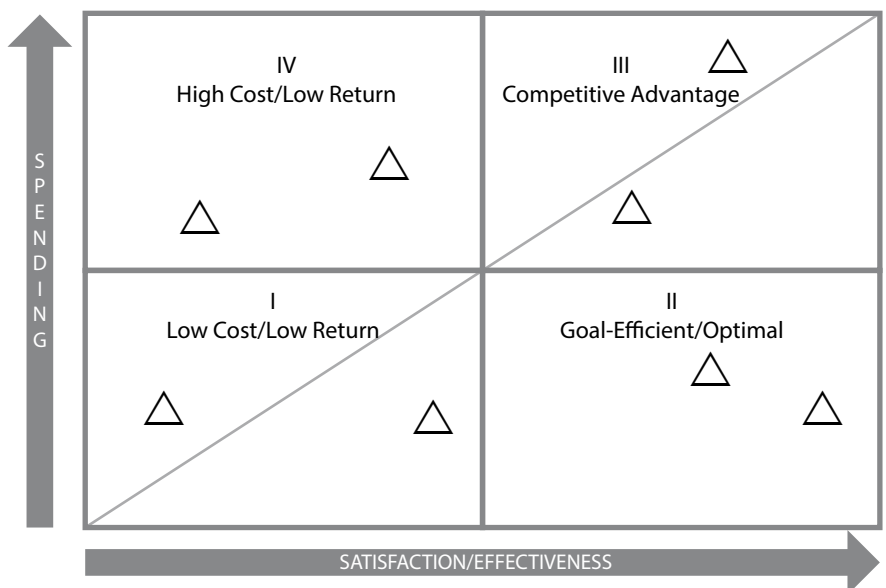
- Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action
- Operational threats and risks, including the control of security, human factors and other activities that affect the organization’s performance, condition or safety
- Factors outside of the organization’s control such as failures in externally supplied (e.g., outsourced) equipment and services
- Security equipment, including replacement, maintenance, information and data management and communications
- Any other threats to the continuity of operations

Please see my article: “Robust, Replicable and Defensible Risk Management—At Headquarters or the Front” in the July-August 2016 issue of *Defense AT&L* magazine.

4. Security Training and Qualification

Security-minded organizations appoint (and entrust) personnel to operate their security management systems. Like any other responsible positions in the military, the people who design, operate and manage the security equipment and processes must be suitably qualified in education, training,

Figure 2. A Cost vs. Effectiveness Matrix (Example)

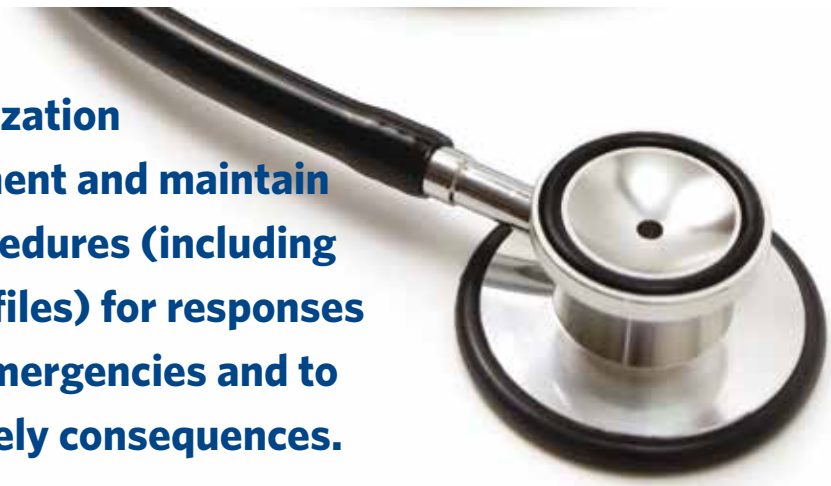


certification and/or experience. I put the word “qualified” in italics because training may not be enough. Commanders need qualification programs—not just a training plan—for all critical positions and watch stations.

Furthermore, all personnel must be fully aware and supportive of the importance of compliance with security management

security management policy, objectives, targets or programs, processes or procedures, and the introduction of new security infrastructure, equipment, or technology also should be documented.

Auditing the supply chain also means auditing compliance with legal, statutory and other regulatory security requirements,



The security-minded organization needs to establish, implement and maintain appropriate plans and procedures (including creating back-up records or files) for responses to security breaches and emergencies and to prevent and/or mitigate likely consequences.

policies and procedures and of the requirements of the Security Management System, as well as their own roles in achieving compliance. This includes emergency preparedness and response, and awareness of the potential security implications of deviating from specified procedures.

5. Supply Chain Security

Every military organization has a supply chain. Security requirements and attendant risks, whether upstream or downstream of its activities, can profoundly affect operations, products or services. Identifying, evaluating and mitigating threats posed from upstream or downstream supply chain activities is just as important as it is for performing the same functions inside your own “fence line.”

Commanders would do well to audit outside that fence line. They can do so by:

- Identifying all links/nodes of the supply chain and ensuring they conform to stated security management policies, controls, and mitigation of unacceptable risks
- Examining documented procedures for situations in which a lack of procedures could lead to failure to maintain operations
- Establishing the security requirements for contractor-furnished goods or services that impact mission accomplishment
- Providing hardened and redundant lines of communication

Where existing designs, installations or operations are changed, documentation should address attendant revisions to command structure, roles or responsibilities. Se-

curity management objectives, delivery of security management programs, and whether the program provides the required level of security (convoys, containers, warehouses, etc.). In my experience, there can be no control of the supply chain without a viable and robust auditing function.

6. Communication and Documentation

Commands must have secure, hardened and redundant procedures for disseminating all pertinent security management information. This applies to outsourced or host nation-provided operations as well as those taking place within the organization. This is especially important when dealing with sensitive or classified information.

A security management system documentation system includes but is not limited to:

- The security management system scope, policy, objectives and targets
- Description of the main components of the security management system and their interaction, with reference to related documents
- Documents such as records the organization determines to be a necessary part of ensuring the effective planning, operation and control of processes related to its significant security risks.

7. Emergency Preparedness and Response

Emergency response may be thought of as conducting normal operations at faster-than-normal speeds—or something entirely different. The security-minded organization needs to establish, implement and maintain appropriate plans and

procedures (including creating back-up records or files) for responses to security breaches and emergencies and to prevent and/or mitigate likely consequences.

Auditing emergency plans and procedures should include all reviewing (and any testing) information that may be required for identified facilities or services during or after incidents or emergencies in order to maintain continuity. The best emergency planning I ever saw was at U.S. Navy Bases along the Gulf Coast, which face an immense and perennial threat from hurricanes. Commanders and staff members periodically should “stress-test” the effectiveness of their emergency preparedness, response and recovery plans and procedures, especially after incidents or emergencies caused by security breaches and threats. They should test these procedures periodically.

A supporting program of internal or outside security audits also confirms whether the organization is complying with relevant legislation and regulations, best practices and the policies and objectives established by higher authorities. Commands need to maintain records of results, findings and required preventive and corrective actions.

Security-minded commanders and staffs can audit their security management plans, procedures and capabilities. Security audits can include periodic reviews, testing, post-incident reports and lessons learned, performance evaluations and exercises. Significant findings and observations, once properly evaluated or gamed, should be reflected in revisions or modifications of policies and procedures.

8. Daily “Quick Looks”

Here are some immediate feedback operational initiatives for forward-thinking and security-minded organizations trying to identify and mitigate (on a daily basis) their vulnerability to exploitation. Develop some checklists, and “check out” the following:

- Intrusion detection systems
- Fences, security lighting, natural barriers
- Closed-circuit TV
- Computer backup systems; “firewalls” against viruses and intrusions
- Roof and ventilation duct accessibility
- Construction materials and thickness requirements
- Installed firefighting systems
- Roads, alleys and storm drains
- Parking areas
- Sewage treatment systems
- Locks, doors and access control
- Identification management (i.e., employees, customers and vendors)
- Utilities (including uninterruptible power systems and emergency generators)
- Safes, desks, filing cabinets, controlled/exclusion areas
- Hazardous materials generation, storage, and management

- Vehicle surveillance and security (including delivery and fuel trucks)
- Proximity of emergency services (i.e., fire departments, medical emergency services, and police)
- Mail and package processing

9. Preventive and Corrective Action

Audit → Nonconformity → P/C Action → Corrected/Improved

Auditors (by any name) discover “nonconformities.” They identify the need for either preventive or corrective action. Top management (we hope) supports the audit findings and initiates preventive or corrective actions and seeks feedback and follow-up to measure the success (or lack thereof) of these actions.


Audits of organizational security are no different than audits of any other management program. In fact, the need for prompt corrective action may be even more critical.

10. Continual Improvement

Continual improvement is the basis and underpinning of the ISO. All processes must be considered ongoing and never at an “end state.” Top management develops a continuous improvement mindset that something can always be improved. Continual improvement of organizational security requires that commanders and staffs review their security management systems at planned and frequent intervals. This is necessary in order to ensure continuing effectiveness in an ever-changing environment. Security audits and reviews should include assessing opportunities for improvement and the attendant need to revise the security management system, including security policies and security objectives, plus threats and risks. Organizations already working with ISO 9000 and ISO 14000 can, with minimal effort, expand internal audits and management reviews to cover security and well as quality and environmental management. See the American Society for Quality website at www.asq.org.

Summary

Information can be exploited in many ways, and auditing organizational security has tremendous potential for experienced commanders and staffs to harden their resources and missions. The opportunities for continual improvement from auditing are as vast as cyberspace and as identifiable as office furniture.

Organizational security must be part of every mission. Outputs from security audits should be the catalyst for any revisions to the security management system, together with cost-benefit analyses, schedules, risk revisions, and other justifications. Establish policies and procedures, identify threats, conduct risk assessments, implement processes, identify corrective actions, and establish a mindset of continual improvement. And audit. 

The author can be contacted at generazz@aol.com.